(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2004 (16.12.2004)

PCT

(10) International Publication Number
WO 2004/109535 A1

(51) International Patent Classification?: G06F 15/173, 15/16, 11/30

(21) International Application Number:
PCT/US2003/017905

(22) International Filing Date: 5 June 2003 (05.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: IPASS INC. [US/US]; 3800 Bridge Parkway, Redwood City, CA 94065 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: SUNDER, Singam [IN/US]; 539 Issac Court, San Jose, CA 95136 (US). EDGETT, Jeff, Steven [US/US]; 151 S. Bernardo #24, Sunnyvale, CA 94086 (US). ALBERT, Roy, David [US/US]; 6529 Fall River Drive, San Jose, CA 95120 (US).

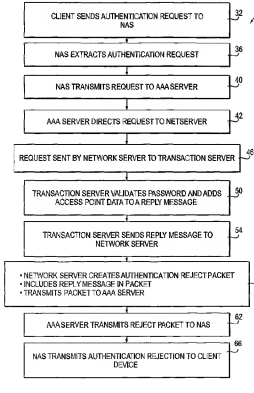
(74) Agent: MARAIS, André, L.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM OF PROVIDING ACCESS POINT DATA ASSOCIATED WITH A NETWORK ACCESS POINT



(57) Abstract: A method of, a system for (Fig. 1), communicating data (Fig. 1, 26) is provided. The method includes receiving an authentication request (Fig. 2, 32, 36) from a client device (Fig. 1, 14) at the access point wherein the access request includes identification credentials. The authentication request is then communicated to an authentication server and data associated with the authentication request is retrieved (Fig. 2, 36). A reply message is communicated to the access point that includes the data and that rejects the authentication request (Fig. 2, 56, 62, 66). The access point may service a wireless hotspot and, thus, a client device in the hotspot may identify the particular hotspot with which it is communicating (Fig. 6, 7).

WO 2004/109535 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM OF PROVIDING ACCESS POINT DATA ASSOCIATED WITH A NETWORK ACCESS POINT

FIELD OF THE INVENTION

The present invention relates generally to a method and system of providing access point data associated with a network access point. The invention extends to a machine-readable medium including a plurality of instructions that cause a computer to carry out the method.

BACKGROUND

So-called "wireless hotspots" are becoming increasingly popular for mobile workers to gain access to computer networks. These hotspots typically allow users to connect to the Internet via their laptops in hotels, airports and cafes in a wireless fashion. There are movements afoot to set up wireless networks just about everywhere you can imagine. These rapidly proliferating wireless nodes or wireless hotspots are typically 802.11b or the like compliant, and are emerging most large cities around the world.

In order to meet the needs of mobile customers, for example using wireless hotspots, Internet Service Providers (ISPs) have begun to offer local-call access to the Internet from various locations world wide, such a service being termed a "roaming" Internet access solution. The requirement for a roaming solution arises primarily because ISPs tend to specialize by geographic area, causing gaps in service coverage. The expansion of network infrastructure, network management and continuous upgrades to meet required reliability and performance standards all place tremendous capital and time burdens on ISPs. For these reason, many ISPs only locate Points of Presence (POPs) in a limited geographic area.

For the reasons set out above, the ability for ISPs to offer Internet roaming solutions, especially to business customers, is becoming increasingly important as many businesses utilize Internet-based communications to replace traditional remote access solutions for their telecommuters and mobile work forces. In order to provide Internet

roaming solutions, some ISPs have begun to share network infrastructure to gain additional geographic reach. A user may then use a connection application to establish a network connection to a network connection point in a wired or wireless fashion.

For the purposes of this specification, the term "connection application" should be construed broadly as including, but not limited to, any device (both hardware and software) including functionality to authenticate data e.g., a peer-to-peer authentication arrangement, a dialer, a smart client, a browser, a supplicant, a smart card, a token card, a PDA connection application, a wireless connection, an embedded authentication client, an Ethernet connection, or the like.

SUMMARY OF THE INVENTION

In accordance with an aspect of the present invention, there is provided a method of communicating data via a network access point to a client device, the method including:

receiving an authentication request from the client device at the access point, the authentication request including identification credentials;

communicating the authentication request to an authentication server;

retrieving data associated with the authentication request; and

communicating a reply message to the network access point, the reply message including the data and at least challenging the authentication request.

The authentication request may include a request identifier that identifies that the request is a faked authentication request. In one embodiment, the method includes communicating the reply message to a connection application on the client device, the reply message including one of an access challenge or an access rejection.

The data may be access point data that identifies a wireless local area network. The method may include communicating the authentication request from the authentication server to a transaction server that selectively identifies the data associated with the request and rejects the authentication request.

In one embodiment, the data includes data selected from at least one of data identifying a geographical location of the access point, time data, data that identifies the

network that the access point forms part of, data identifying if a user is permitted to use the access point, data relating to the quality of service of the access point, data indicating a pending electronic message, and data indicating pending electronic mail.

The access point may provide network access at a wireless hotspot. The authentication request may be associated with a roaming access service provider.

Further in accordance with the invention, there is provided a method of obtaining data via a network access point with which a client device communicates, the method including:

communicating an authentication request from the client device at the network access point, the access request including user credentials and a request identifier to identify that the authentication request is a faked authentication request;

receiving a reply message from the network access point that at least challenges access to the network but includes the data; and

processing the reply message to extract the data.

The method of may include generating a user interface that displays the data to a user of the client device.

The invention extends to a machine-readable medium embodying a sequence of instructions that, when executed by the machine, cause the machine to execute any of the methods described herein.

Still further in accordance with the invention, there is provided a computer system, which includes:

at least one network access point to receive an authentication request from a client device at the network access point, the authentication request including identification credentials; and

at least one server to receive the authentication request from the network access point, wherein data associated with the authentication request is retrieved and communicated in a reply message to the network access point, the reply message at least challenging the authentication request.

The invention extends to a client device to obtain data via a network access point with which the client device communicates, the client device including:

a communication interface to communicate an authentication request from the client device to a the network access point, the access request including user credentials and an identifier to identify that the authentication request is a faked authentication request, and to receive a reply message from the network access point; and

a processor to process the reply message to extract the data.

Other features and advantages of the present invention will be apparent from the drawings and detailed description that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not intended to be limited by the figures of the accompanying drawings, in which:

Figure 1 is a schematic diagram of an exemplary embodiment of a system, in accordance with an aspect of the present invention, for determining access point data using a computer network;

Figure 2 shows a block diagram of a method, also in accordance with an aspect of the present invention, for determining access point data using a computer network;

Figure 3 is a schematic diagram of a further exemplary embodiment of a system, in accordance with an aspect of the present invention, for determining access point data using a computer network;

Figure 4 is a schematic representation of a transaction server of the system of Figure 1;

Figure 5 is a schematic representation of an exemplary roaming access service provider network;

Figures 6 and 7 are schematic representations of graphic user interfaces generated by the method of **Figure 2**; and

Figure 8 is a schematic diagram of a computer system, which may be configured as a client device or configured to function as any one of the servers herein described.

DETAILED DESCRIPTION

A method and system communicating data via a network access or connection point is described. The access data may, for example, include location information that identifies the geographical location of the access point.

BACKGROUND

Network access devices typically encrypt a network user credential, such as a password, input by a network user to authorize access to a network by the user. In order to enhance security, the network access device may encrypt the network user credential with a public key, which is part of a public/private key pair, prior to transmitting the encrypted network password to a network decryption server. The network decryption server then decrypts the network user credential using the private key of the public/private key pair, where after the decrypted password is sent to an Authentication Authorization and Accounting (AAA) server for verification. If the password is positively verified at the AAA server, the AAA server sends an appropriate acknowledgment signal to the network access device indicating that the password has been properly verified or authenticated. Based on the acknowledgement signal, the network access device gains access to the Internet or some other resource. Once access is provided, updated data may then be downloaded to the network access device. For example, a connection application running on the network access device may have its phonebook updated with pricing data, connection quality data or the like that may have changed for one or more connection points (POPs) in the phonebook. The prior art, however, requires network access prior to the connection application obtaining any data about the access point.

ARCHITECTURE

Referring in particular to Figure 1 of the drawings, reference numeral 10 generally indicates high-level architecture of a system, in accordance with one embodiment of the invention, for providing access point data associated with a access point of a network access server (NAS) or access gateway 12 which defines an access gateway to a client device 14. The client device 14 may be in the form of a mobile

computing device such as laptop computer, PDA, or the like. The client device 14 includes a connection application 16 for establishing a connection to an external computer network. For example, the connection application 16 may, via the NAS 12, provide a mobile user access to the Internet 18. As described in more detail below, the system 10 further includes an Authentication, Authorization and Accounting (AAA) server 20, a network server 22 (NetServer), and a transaction server 24.

As mentioned above, the connection points such as the NAS 12 may be provided in a large number of diverse locations such as in coffee shops, hotels, in airport buildings and any other place that may or may not be open to the public. In one embodiment, wireless access may be provided by a NAS 12 located at each of these locations. It is however to be appreciated that the access point may be a wired or wireless access point.

ROAMING ACCESS SERVICE PROVIDERS

Roaming access service providers allow global connectivity services that give mobile users access to the Internet from a plurality of locations often referred to as hotspots. Users or customers of a roaming access service provider utilize the client connection application 16 to connect to a computer network such as the Internet 18. In one embodiment, the user may specify an access type and location from an intuitive user interface, and select a local connection point. The connection application 16 may then transmit the user authentication request to the roaming access service provider's network and a connection to the Internet 18 may be established if the authentication request succeeds. The invention described herein however, enables determining the details of the access point prior to authenticating. In some embodiments, an access point 13 may be remotely located from the NAS 12. The client device 14 may then communicate with the NAS 12 via the access point 13 which may service a wireless hotspot 15.

The connection application 16 may include a list of access points that are within the roaming access service provider's network. The connection application 16 may also include detailed information about connection technology, pricing, and location details

for each network access point. The network access point and its associated information may be grouped together in a directory interface, for example, a so-called phonebook. Users of the connection application 16 may utilize the directory information when deciding to establish a connection to the Internet 18. The connection application 16 may automatically update the directory information when connecting to the Internet 18.

The directory information in the connection application 16 typically contains static information that can only be updated after the client device 14 connects to the Internet 18. The static nature of the directory information may, however, be undesirable in certain circumstances.

For example, a roaming access service provider may support multiple pricing plans. When a contract is negotiated and a customer is provisioned, each customer may be assigned a pricing plan. The directory interface may include a price paid by the customer for utilizing the roaming access service provider's service. Static pricing information contained in the directory may be sufficient for most of the pricing plans, but for certain plans like pre-paid, daily fixed rate etc, it may necessary to show additional, dynamic pricing information to the user. Examples of such information include an amount left in user's account (e.g. in a pre-paid scenario), a number of minutes remaining in the day (e.g. in a daily fixed rate scenario), or the like.

The location information in the directory may include details of various geographical locations such as a site name, a site telephone phone number, a site address, a city name in which the site is located, a state or region name, a country code, Greenwich Meantime (GMT) offset, or the like. The connection application 16 may be able automatically to detect the presence of the wireless (e.g. 802.11a/802.11b or any Wi-Fi link) access points (using NDIS 5.1 (Network Driver Interface Specification) OIDS (Object Identifiers)) and associate them to the directory entry using a SSID (Service Set Identifier) used by the access point. The SSID is a 32 character unique identifier attached to the header of data packets sent over a Wireless Local Area Network (WLAN) that acts as an identifier when a mobile device attempts to connect to the basic network. The SSID differentiates one WLAN from another and thus may act as a connection point

identifier. Thus, the SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

Unfortunately, network providers tend to use the same or a small set of SSIDs over their entire network even though the connection points in various hotspots are geographically dispersed. The use of the same SSID at geographically dispersed locations or different hotspots does not impair operation from a network provider's point of view, as the SSIDs are only required to be unique within the hotspot itself. Thus, different hotspots can have the same SSID and thus may not assist a user in identifying the particular geographical location of the actual hotspot in which he is located. As the SSID may not be unique to the hotspot, the connection application cannot associate these SSIDs to a unique directory entry (associated with a specific geographical location) because more than one entry in the directory may have a matching SSID.

METHODOLOGY

When a user with the mobile client device 14, that is equipped with a wireless interface 26, enters an area serviced by the NAS 12, typically known as a wireless hotspot, the wireless connection may establish a local wireless connection. The local connection may use 802.11a, 802.11b, or the like protocol. Such a connection merely establishes a connection between the client device 14 and the NAS 12 (or the access point 13 in another embodiment) and does not in itself provide access to any external network such as the Internet 18. In order to gain access to any external network, a user typically requires authentication, as described above. However, granting access to an external network may result in cost implications and, thus, the user may require an indication of costs that may arise prior to authentication. In order to do this, the connection application 16 may require access data on the connection point or NAS 12. As mentioned above, the SSID of the wireless access point or NAS 12 may not uniquely identify the NAS 12.

However, the connection application 16 may invoke a method 30 (see Figure 2), in accordance with one aspect of the invention, of determining access point data

associated with the access or connection point. As shown at block 32, the connection application 16 on the client device 14 sends an authentication request 34 (see Figure 1) to the NAS 12. The authentication request 34 may include predetermined credentials associated with the customer or user of the client device 14. In one embodiment, in order to obtain data that may be relevant to a user of the client device 14, the client device fakes or feigns an authentication request that the access point communicates to an authentication server. The authentication server may then identify that the request is a fake request and send a reply message to the client device including data associated with the user (e.g., associated with a user credential), as described in more detail below. It is to be appreciated that the data communicated need not be limited to access point data but may include any data which is communicated to the client device 14 prior to granting the device 14 access to a network. The data may include, for example, data identifying a geographical location of the access point, time data, data that identifies the network that the access point forms part of, data identifying if a user is permitted to use the access point, data relating to the quality of service of the access point, data indicating a pending electronic message, and/or data indicating pending electronic mail.

The credential may be user identification data. For example, the connection application 16 may use

RoamingServiceProvider/<ConnectionApplicationId>-<Timestamp>@DiscoverLocation

as an exemplary user name. The ConnectionApplicationId may define the user identification data (for example a connect dialer identification associated with the customer or the client when this data is available). The Timestamp may be the current system time and the DiscoverLocation may define a location or realm identifier to indicate that the client device 14 is requesting access point data (e.g. at a hotspot) and not requesting a connection to the external network.

The connection application 16 may build a password using the contents of a username. In some embodiments, the connection application 16 can also include information about the access point or NAS 12 determined through NDIS 5.1 OIDS in an

authentication request. An example of such information includes the MAC address of the access point or NAS 12. The MAC address may optionally be included in the authentication request as the transaction server (discussed below) may utilize the MAC address of the access point to determine the geographical location of a hotspot using a database whereby access points are mapped to a location.

As mentioned above, the connection application 16 may transmit the authentication request 34 to the NAS 12 of the network service provider or the access gateway using an appropriate communication protocol. For example, the connection application 16 may support the following protocols:

PPP (Point-to-Point, which may be used for dial access points);

GIS (Generic Interface Specification, which may be used for wired and wireless broadband access points that may require HTTP or HTTPS based authentication); and

802.1x (Port based network access control, which is an emerging standard for Wired and Wireless Broadband Access points).

The network provider's NAS or access gateway 12 may extract the authentication request (see block 36 in Figure 2) and transmits the authentication request to the AAA server 20 as shown by arrow 38 in Figure 1 (see also block 40 in Figure 2). The AAA server 20 may be a local server and, in one embodiment, RADIUS protocol may be used for this communication.

The AAA server 20, of the particular network provider, may determine that the request should be routed to a network of the roaming access service provider. In particular, based on a roaming access service provider's prefix to the authentication request, the AAA server 20 may route the authentication request to the network server 22 of the roaming access service provider (see block 42 in Figure 2 and arrow 44 in Figure 1). The network server 22 may then receive the authentication request (e.g., sent using RADIUS protocol), establish an Secure Sockets Layer (SSL) tunnel to the transaction server 24, and transmit the request to the transaction server 24 via the proprietary protocol of the roaming access service provider (as shown block 46 and arrow 48).

Upon receipt of the request, the transaction server 24 identifies the authentication request, validates the user credentials (e.g. password) and adds the access point or location data (see block 50). The access point data may include geographical location information, pricing details, GMT time at the server and the GMT offset of the access location to a reply message that it generates. In addition, the transaction server rejects 24 the authentication request and transmits the reply message (see arrow 52 and block 54) to the network server 22. The authentication request is rejected by the transaction server 24 so that the NAS or access gateway 12 does not provide network access (e.g. Internet access) to the client device 14. The client device 14, as mentioned above, uses the method 30 to obtain access point data in this mode of operation and thus the request need not be approved.

As shown at block 56, upon receipt of the reply message, the network server 22, creates an authentication reject packet (e.g. a RADIUS packet), includes the reply message in the packet, and transmits the packet to the AAA server 20 of the network service provider (see block 56 and arrow 58). The network service provider's AAA server 20 may then proxy the authentication reject packet to the NAS or the access gateway 12 as shown by arrow 60 (see also block 62). The NAS or access gateway 12 then, as shown by arrow 64, transmits the authentication rejection to the connection application 16 via an appropriate protocol (see also block 66). The exemplary protocols identified above (PPP, GIS, 802.1x or the like) may carry the reply message from the RADIUS packet back to the connection application 16.

The connection application 16 may then parse the reply message to extract the access point data. For example, the connection application 16 may obtain information regarding the geographical location 67 (see Figure 7) of the access point, pricing details 69 associated with use of the particular access point, GMT time at the server, the GMT offset of the access location, or the like.

It will be appreciated that the implementation described above illustrates one exemplary embodiment of the invention. A further exemplary embodiment is shown in Figure 3 which shows a high-level architecture of a system 70, in accordance with an aspect of the invention, for providing access point data associated with an access point

of a network access server (NAS). The system 70 resembles the system 70 and, accordingly, like reference numerals have been used to indicate the same or similar features, unless otherwise indicated.

In the system 70, the connection application 16 is replaced by a generic connection client 72 that may not have been customized by a roaming access service provider. In this embodiment an authentication request received from the connection application client 72 is not transmitted to a network server or transaction server as in the case of the system 10.

In the system 70, the authentication request is communicated to the AAA server 20 in a similar fashion to that described above (see arrows 34 and 38 in Figure 3, and blocks 32, 36 and 40 in Figure 2). However, unlike the system 10 where the transaction server 24 terminates the request, in the system 70 the AAA server 20 terminates the request. The network provider, via its associated AAA server 20, then adds the access point data in a reply message when rejecting the authentication request. As discussed above, the reply message is then communicated back to the client device 14 (see arrows 60 and 64 in Figure 3, and blocks 62 and 66 in Figure 2).

In another alternative implementation, the transaction server 24 includes a challenge to the authentication request instead of rejecting the authentication request. The client device 14 receives the challenge and uses the method 30 to obtain access point data. The client device 14 can then send a subsequent fake authentication request to the transaction server 24. This scheme of the client transmitting an authentication request followed by the transaction server replying with an access challenge can be repeated multiple times . The exchange of messages may eventually end when the transaction server finally rejects the authentication request. This mechanism can be used for transmitting more information between the client and the transaction server 24.

Returning to the system 10, its various components are now discussed in more detail.

Transaction Server

In one embodiment, the transaction server 24 includes a server subsystem 76, a cache subsystem 78 and a handler subsystem 80. The server subsystem 76 may be responsible for receiving requests, maintaining a queue of requests, and managing handlers that process the requests from the network server 22. Major components of server subsystem 76 may include a listener component 82, a receiver component 84, a message queue component 86, and a handler component 88. The listener component 82 may receive the HTTPS requests from the network server 22 on a TCP/IP port and pass the requests to the receiver component 84.

The receiver component 84 determines the type of request from the network server 22. For example, the request may be a control request (e.g. shutdown/dump queue) or a data request (e.g. authentication/accounting). If a control request is received the appropriate control action is then initiated. If data request is received, the receiver component 84 may then add the request to a message queue of the message queue component 86. Thereafter, the message queue component 86 may notify worker threads of the handler component 88 when a new request is added to a message queue. If a worker thread is available to process a request, it removes the request from the message queue and processes it immediately using an encapsulated handler. However, if a worker thread is not available to process a request, the request remains in the message queue waiting for one of the worker threads to finish its processing and process the pending request.

The cache subsystem 78 provides a set of entity objects for use by the handler subsystem 80. The cache subsystem 78 retrieves information stored in databases and caches it in memory. In one exemplary embodiment, the cache subsystem 78 includes a customer cache component 90, a policy cache component 92, a domain cache component 94, a routing cache component 96, and a location cache component 98. The cache components 90 to 98 retrieve information stored in the databases and cache it using a cache manager 100. The cache components 90 to 98 maintain the integrity of the caches by monitoring changes to the data in the database. When the cached data is invalidated by a change in the database, the cache components 90 to 98 refresh the data from the database.

In one embodiment, the handler subsystem 80 provides business logic needed to process the authentication and accounting messages and thus includes an authentication component 102 and an accounting component 104. The handler subsystem 80 may process the authentication and accounting requests received by a handler information thread. The details of the handler subsystem 80 are described below.

The authentication handler component 102 may process all authentication requests from the network server 22. The authentication handler component 102 may validate a source from which an authentication request is received, selectively authorize roaming access through a policy manager, resolves the route to a RoamServer 110 (discussed below with reference to Figure 5), and transmit an authentication request to the RoamServer 110. The RoamServer 110 may then authenticate the request against the local AAA server 20, and transmits the authentication result back to the authentication handler component 102. The authentication handler component 102 may transmit the authentication result in the form of the reply message to the network server 22. In certain embodiments, the authentication handler component 102 uses the customer and routing cache components 90, 96 respectively to validate the request and to determine the route to the RoamServers 110.

If the authentication handler component 102 receives an authentication request to determine access point data (which may be called a "discover location request"), as described above, then the request may not be forwarded to the RoamServer 110. In one embodiment, a password included in the request is validated using an appropriate algorithm. Once the authentication handler component 102 determines that the request is a valid discover location request, it then identifies the location of the connection or access point hotspot 15 using the location cache component 98. In one embodiment, access point locations are represented in RADIUS requests in a variety of ways. The location cache component 98 may implement provider specific business rules to determine a location type for a given record.

During the resolution process to obtain the geographical location of the access point, if the location resolves to a known location identifier then the corresponding time

zone information (time_zone_info) may be looked up, and the GMT offset of the location may be determined. The authentication handler may add location description data (location_description), location identification data (location_group_id), GMT time data of the transaction server 24 (gmt_time), and a GMT offset (gmt_offset) to the reply packet in the reply message attribute in the following exemplary format.

Location=San Francisco, CA, US;LocationGroupId=1038; GMTTime=2002-08-15 23:12:34;GMTOffset=36000

The reply status indicating that the authentication has been rejected is then transmitted to the network server 22.

Connection Application

The connection application 16 on the client device 14 includes a location interface 106 and access point data interface 108 (see Figures 6 and 7) and embedded Application Program Interface (eAPI) components. The eAPI components provide a core set of Component Object Model (COM) API calls. The core API calls are organized into independent COM interfaces including POP, connect, and location interfaces.

The access point data interface 108 (POP interface) may provide APIs for determining details of a directory of access points. These APIs may be used to filter and query access points from the directory. The location interface 106 (connect interface) may provide APIs for connecting to an access point. Using these APIs, the connection application 16 can establish an Internet connection to dial, wired and wireless access points.

The location interface 106 may provide APIs for determining the details 114 of the geographical or physical location of an access point. This information may be returned from the transaction server 24 as a result of a discover location authentication request that identifies that the user of the client device 14 desires access point data. The location group identifier present in the reply can be used to associate the location object to the access points object returned by the POP module.

Exemplary API Calls used by the connection application

Exemplary API calls to support the connection application 16 in determining access point data, for example the geographical location of the access point, are set out below.

ConnectApp::DiscoverLocation

This API may initiate the location discovery process. In certain embodiments, this is an asynchronous call, which posts a message when the information is available to be retrieved with GetDiscoveredLocation().

HRESULT DiscoverLocation([in] _HWND hWnd, [in] long nMessageID)

Parameters,

hWnd

[in] Window handle that will receive a message when location information is available.

nMessageID

[in] Message ID to send to identify that location information is available.

ppLocation

[out, retval] A reference to the IiPassLocation object.

Return Values

RASP_SUCCESS

Indicates that the API execution to the roaming access service provider (RASP) was successful.

RASP_IN_PROGRESS

Indicates that the discover location thread has already been started.

RASP_FAIL

Indicates that the discover location thread could not be created.

When the location discovery process is complete, the message nMessageID is posted to the window hWnd. In one exemplary embodiment, wParam has one of the following values:

wParam	Description
0	Location information is now ready to be retrieved via GetDiscoveredLocation().
1	Location discovery thread is already in progress.
2	Cannot create location discovery thread.
3	Location discovery failed. Possible causes include: user is already authenticated reply message did not contain all required location parameters (location, locationgroupid, gmttime, gmtoffset)

In one embodiment, the call creates a thread and returns immediately to the access point data requestor. To discover the location, the thread may use a normal authentication request with the following special values:

Username: RoamingServiceProvider/<ConnectionApplicationId>-<Timestamp>@DiscoverLocation

The ConnectionApplicationId may define the user identification data (for example a connect dialer identification associated with the customer or the client when this data is available).

The DiscoverLocation may define a realm identifier to indicate that the client device 14 is requesting access point data (e.g. at a hotspot) and not requesting a connection to the external network.

<Timestamp> may be the current time on the client (time_t), printed as an unsigned decimal number. In response to this request, the transaction server 24 may return the access reject message (that includes the location information connection point data) in a reply message in the following exemplary format:

<ReplyMessege>

Location=San Francisco, CA, US;LocationGroupId=1038; GMTTime=2002-08-15 23:12:34;GMTOffset=36000

</ReplyMessege>

The following conditions are applicable to the exemplary reply message information:

GMT time format may be yyyy-mm-dd hh:mm:ss

GMT time offset format may be in seconds

The difference between the GMT time and the time on the client device 14 may be recorded. The difference may then be used in the future to produce output values for GetGMTTime() and GetLocalTime().

RASPConnect::GetDiscoveredLocation

This API retrieves the location information that was obtained with DiscoverLocation(), as described above.

HRESULT GetDiscoveredLocation([out, retval] IRASPLocation **ppLocation)

Parameters

ppLocation

[out, retval] A reference to the IRASPLocation object.

Return Values

RASP_SUCCESS

Indicates that the API execution is successful.

RASP _FAIL

Indicates that discover location request failed.

IRASPLocation::GetLocation

Gets the location name.

HRESULT GetLocation([out, retval] BSTR *pLocation)

Parameters

pLocation

[out, retval] Location name from the location object. On successful execution, the server may allocate the memory and it may be a client's responsibility to free this memory.

Return Values

RASP _SUCCESS

Indicates that the API execution is successful.

IRASPLocation::GetLocationGroupID

Gets the location group ID.

HRESULT GetLocationGroupID([out, retval] BSTR *pLocationGroupID)

Parameters

pLocationID

[out, retval] Location group ID from the location object.

Return Values

RASP _SUCCESS

Indicates that the API execution is successful.

IRASPLocation::GetGMTOffset

Gets the GMT offset from the location object.

HRESULT GetGMTOffset([out, retval] long *pnGmtOffset)

Parameters

pnGmtOffset

[out, retval] GMT offset for this location. The offset value is in seconds.

Return Values

RASP _SUCCESS

Indicates that the API execution is successful.

IRASPLocation::GetGMTTime

Gets the current GMT time, as determined from the location object.

HRESULT GetGMTTime([out, retval] time_t *pnGMTTime)

Parameters

pnGMTTime

[out, retval] GMT time, as computed from transaction server. time_t may be the number of seconds since January 1, 1970.

Return Values

RASP _SUCCESS

Indicates that the API execution is successful.

In certain embodiments, when a location object is created, the difference between GMT time and system time may be recorded. This difference may then be used in the future to calculate the GMT time based on the current system time.

RASPLocation::GetLocalTime

Gets the current local time, as determined from the location object.

HRESULT GetLocalTime([out, retval] time_t *pnLocalTime)

Parameters

pnLocalTime

[out, retval] Local time, as computed from transaction server. time_t may be the number of seconds since January 1, 1970.

Return Values

RASP _SUCCESS

Indicates that the API execution was successful.

In certain embodiments, this is a convenience function, which takes GetGMTTime, and applies the GetGMTOffset to it.

IRASPLocation::GetPOP

This API may get the POP object corresponding to this location object.

HRESULT GetPOP([out, retval] IiPassPOP *pPop)

Parameters

pPop

[out, retval] The POP object associated with this location.

Return Values

RASP _SUCCESS

Indicates that the API execution was successful.

This method may use the location ID to retrieve the POP information from the directory. In certain embodiments, only POP fields that can be uniquely identified may include contain a value in the returned POP object. Other fields may be 0 or NULL.

In certain embodiments, GetPOP() API may perform the directory search to create the POP object when it is called, not when the InitRASPLocation object is created. Once created, the POP object may be cached for future calls to GetPOP() for this location object.

RASPPOP::GetPOPLocationGroupID

This API may get the location group ID of the access point.

HRESULT GetPOPLocationGroupID([out, retval] BSTR *pLocationGroupID)

Parameters

pLocationGroupID

[out, retval] Returns the location group ID.

Return Values

RASP _SUCCESS

Indicates that the API execution was successful.

IRASPPOP::GetPOPTimeDayStarts

This API may get a local start time for a 24-hour billing cycle.

HRESULT GetPOPTimeDayStarts([out, retval] BSTR *pTimeDayStarts)

Parameters

pTimeRateStarts

[out, retval] Returns the local time of the start of the billing cycle. The value returned will be in 24-hour format (i.e. 18:00:00).

Return Values

RASP _SUCCESS

Indicates that the API execution was successful.

Referring in particular to Figure 5, reference numeral 112 generally indicates an example of the invention applied in a roaming access system that provides roaming Internet access in a relatively secure manner. When a roaming user, shown to be a subscriber to a "home" ISP 114, connects to a remote ISP 116 that provides a local POP 118 within a specific geographic area 120 (which may service a hotspot 15), the roaming user inputs the same user name 122 and password 124 (authentication data or user credentials) used when connecting via a POP 128 of the "home" ISP 114.

As mentioned above, the hotspot 15 may be any location (e.g., cafe, hotel, airport, or the like) where a network access point is provided to connect to a computer network. In the exemplary embodiment shown in Figure 5, is within the hotspot 15, the method described herein may be used to identify the particular hotspot 15. Once the hotspot 15 has been identified, the connection application 16 may provide the user with, for example, details regarding use of the hotspot 15 in accordance with a contract entered into with the home ISP 114. For example, a directory interface may include a

price paid by the user for utilizing the roaming access service provider's service at the hotspot 15. Further, once the hotspot 15 has been identified, dynamic pricing information relating to pre-paid access, daily fixed rate access, or the like may be presented to the user. Examples of such information include an amount left in user's account (e.g. in pre-paid scenario), a number of minutes remaining in the day (e.g. in daily fixed rate scenario) or the like. It is however to be appreciated that, in one embodiment of the invention, the method and system can communicated any data to the user without actually authenticating the user.

Figure 8 shows a diagrammatic representation of machine in the exemplary form of a computer system 200 within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines, in a networked deployment, the machine may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

The exemplary computer system 200 includes a processor 202 (e.g., a central processing unit (CPU) a graphics processing unit (GPU) or both), main memory 204 and static memory 206, which communicate with each other via a bus 208. The computer system 200 may further include a video display unit 210 (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)). The computer system 200 also includes an alphanumeric input device 212 (e.g., a keyboard), a cursor control device 214 (e.g., a mouse), a disk drive unit 216, a signal generation device 218 (e.g., a speaker) and a

network interface device 220. The disk drive unit 216 includes a machine-readable medium 222 on which is stored one or more sets of instructions 224 (e.g., software) embodying any one or more of the methodologies or functions described herein. The software 224 may also reside, completely or at least partially, within the main memory 204 and/or within the processor 202 during execution thereof by the computer system 200, the main memory 204 and the processor 202 also constituting machine-readable media.

The software 224 may further be transmitted or received over a network 226 via the network interface device 220. While the machine-readable medium is shown in an exemplary embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-readable medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present invention. The term "machine-readable medium" shall accordingly be taken to included, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals.

Thus, a method of, and system for, obtaining and providing data prior to authentication is described. In the foregoing detailed description, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader scope and spirit of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method of communicating data via a network access point to a client device, the method including:

receiving an authentication request from the client device at the access point, the authentication request including identification credentials;

communicating the authentication request to an authentication server;

retrieving data associated with the authentication request; and

communicating a reply message to the network access point, the reply message including the data and at least challenging the authentication request.

2. The method of claim 1, wherein the authentication request includes a request identifier that identifies that the request is a faked authentication request.

3. The method of claim 1, which includes communicating the reply message to a connection application on the client device, the reply message including one of an access challenge or an access rejection.

4. The method of claim 1, wherein the data is access point data that identifies a wireless local area network.

5. The method of claim 1, which includes communicating the authentication request from the authentication server to a transaction server that selectively identifies the data associated with the request and rejects the authentication request.

6. The method of claim 1, wherein the data includes data selected from at least one of data identifying a geographical location of the access point, time data, data that identifies the network that the access point forms part of, data identifying if a user is permitted to use the access point, data relating to the quality of service of the access

point, data indicating a pending electronic message, and data indicating pending electronic mail.

7. The method of claim 1, wherein the access point provides network access at a wireless hotspot.

8. The method of claim 1, wherein the authentication request is associated with a roaming access service provider.

9. A method of obtaining data via a network access point with which a client device communicates, the method including:

communicating an authentication request from the client device at the network access point, the access request including user credentials and a request identifier to identify that the authentication request is a faked authentication request;

receiving a reply message from the network access point that at least challenges access to the network but includes the data; and

processing the reply message to extract the data.

10. The method of claim 9, which includes generating a user interface that displays the data to a user of the client device.

11. The method of claim 10, wherein the data includes data selected from at least one of data identifying a geographical location of the access point, time data, data that identifies the network that the access point forms part of, data identifying if a user is permitted to use the access point, data relating to the quality of service of the access point, data indicating a pending electronic message, and data indicating pending electronic mail.

12. The method of claim 9, wherein a connection application provided on the client device generates the faked authentication request that identifies that the client device is requesting data from the network access point.

13. The method of claim 9, wherein communicating the authentication request from the client device is via a wireless communication link.

14. A machine-readable medium embodying a sequence of instructions that, when executed by the machine, cause the machine to:

receiving an authentication request from a client device at a network access point, the authentication request including identification credentials;

communicate the authentication request to an authentication server;

retrieve data associated with the authentication request; and

communicate a reply message to the network access point, the reply message including the data and at least challenging the authentication request.

15. The machine-readable medium of claim 14, wherein the authentication request includes a request identifier that identifies that the request is a faked authentication request.

16. The machine-readable medium of claim 14, wherein the reply message is communicated to a connection application on the client device.

17. The machine-readable medium of claim 14, wherein the data is access point data that identifies a wireless local area network.

18. The machine-readable medium of claim 14, wherein the authentication request from the authentication server is communicated to a transaction server that selectively identifies the data and rejects the authentication request.

19. The machine-readable medium of claim 14, wherein the authentication request is associated with a roaming access service provider.

20. A machine-readable medium embodying a sequence of instructions that, when executed by the machine, cause the machine to:

communicate an authentication request from a client device to a network access point, the access request including user credentials and an identifier to identify that the authentication request is a faked authentication request;

receiving a reply message from the network access point that at least challenges access to the network but includes the data; and

processing the reply message to extract the data.

21. The machine-readable medium of claim 20, wherein a user interface is generated that displays the data to a user of the client device.

22. The machine-readable medium of claim 21, wherein a connection application provided on the client device generates the faked authentication request that the client device is requesting data from the network access point.

23. The machine-readable medium of claim 20, wherein the communicating the authentication request from the client device is via a wireless communication link at a wireless hotspot.

24. A computer system, which includes:

at least one network access point to receive an authentication request from a client device at the network access point, the authentication request including identification credentials; and

at least one server to receive the authentication request from the network access point, wherein data associated with the authentication request is retrieved and communicated in a reply message to the network access point, the reply message at least challenging the authentication request.

25. The system of claim 24, wherein the authentication request includes a request identifier that identifies that the request is a faked authentication request.

26. The system of claim 24, wherein the reply message is communicated to a connection application on the client device.

27. The system of claim 25, wherein the data is access point data that identifies a wireless local area network.

28. The system of claim 27, wherein the authentication request is communicated to an authentication server and to a transaction server that selectively identifies the access point data and rejects the authentication request.

29. The system of claim 24, wherein the data includes data selected from at least one of data identifying a geographical location of the access point, time data, data that identifies the network that the access point forms part of, data identifying if a user is permitted to use the access point, data relating to the quality of service of the access point, data indicating a pending electronic message, and data indicating pending electronic mail.

30. The system of claim 24, wherein the access point provides network access at a wireless hotspot.

31. The system of claim 25, wherein the authentication request is associated with a roaming access service provider.

32. A client device to obtain data via a network access point with which the client device communicates, the client device including:

a communication interface to communicate an authentication request from the client device to a the network access point, the access request including user credentials and an identifier to identify that the authentication request is a faked authentication request, and to receive a reply message from the network access point; and

a processor to process the reply message to extract the data.

33. The client device of claim 32, which includes a user interface that displays the data to a user of the client device.

34. The client device of claim 33, which includes a connection application to generate the faked authentication request.

35. The client device of claim 32, wherein the communication interface is a wireless communication link.

36. A computer system, which includes:

means for receiving an authentication request from a client device at a network access point, the authentication request including identification credentials;

means for communicating the authentication request to an authentication server;

means for retrieving data associated with the authentication request; and

means for communicating a reply message to the network access point, the reply message including the data and at least challenging the authentication request.

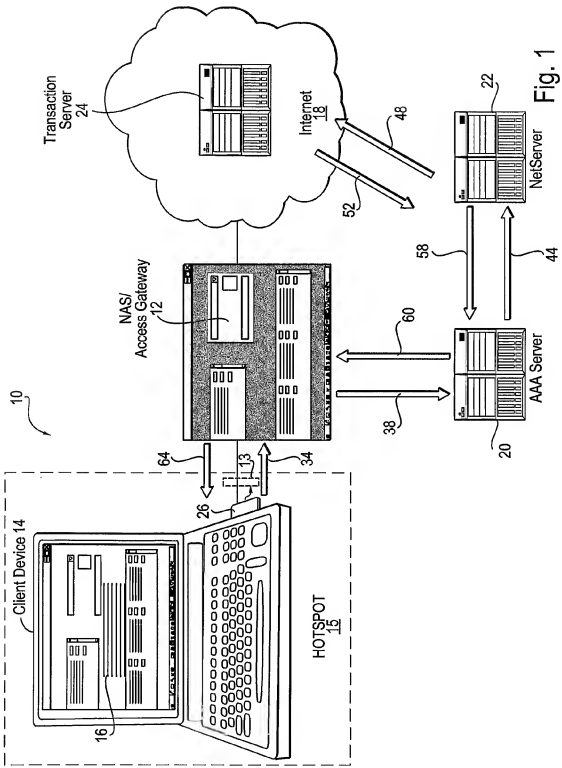

Transaction Server 24
Internet 18
22
NetServer
48
52
58
44
NAS/ Access Gateway 12
60
AAA Server
38
20
10
64
13
34
26
Client Device 14
HOTSPOT 16
16

Fig. 1

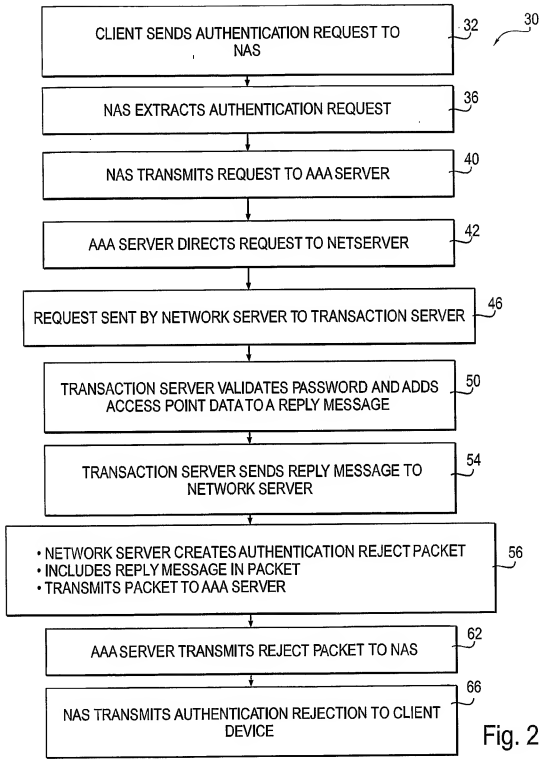

CLIENT SENDS AUTHENTICATION REQUEST TO NAS
32
30
NAS EXTRACTS AUTHENTICATION REQUEST
36
NAS TRANSMITS REQUEST TO AAA SERVER
40
AAA SERVER DIRECTS REQUEST TO NETSERVER
42
REQUEST SENT BY NETWORK SERVER TO TRANSACTION SERVER
46
TRANSACTION SERVER VALIDATES PASSWORD AND ADDS ACCESS POINT DATA TO A REPLY MESSAGE
50
TRANSACTION SERVER SENDS REPLY MESSAGE TO NETWORK SERVER
54
• NETWORK SERVER CREATES AUTHENTICATION REJECT PACKET
• INCLUDES REPLY MESSAGE IN PACKET
• TRANSMITS PACKET TO AAA SERVER
56
AAA SERVER TRANSMITS REJECT PACKET TO NAS
62
NAS TRANSMITS AUTHENTICATION REJECTION TO CLIENT DEVICE
66

Fig. 2

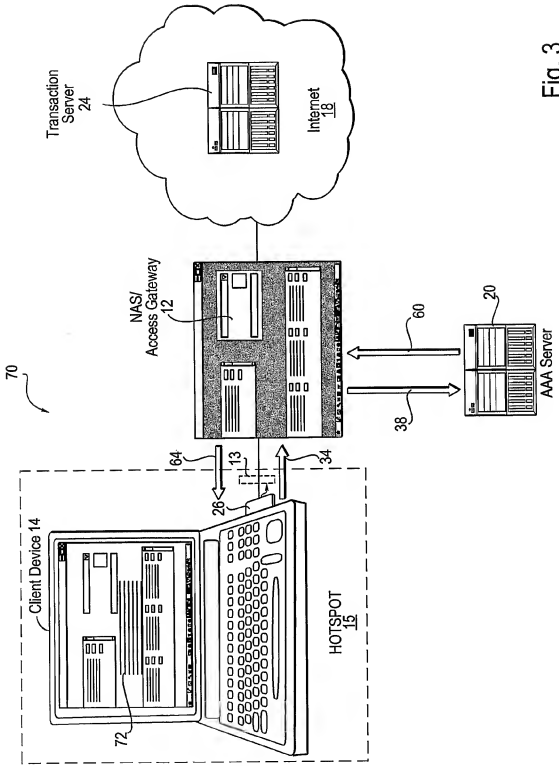

Transaction Server 24
Internet 18
NAS/ Access Gateway 12
70
60
20
AAA Server
38
64
13
34
26
Client Device 14
HOTSPOT 16
72

Fig. 3

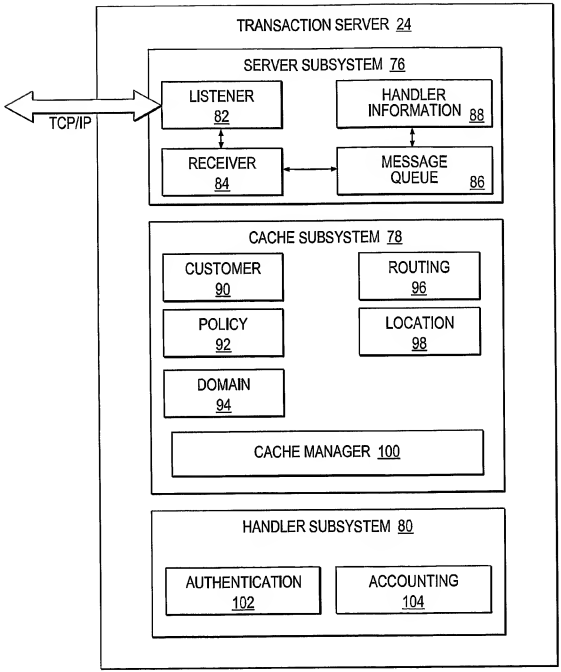

TRANSACTION SERVER 24
SERVER SUBSYSTEM 76
TCP/IP
LISTENER 82
HANDLER INFORMATION 88
RECEIVER 84
MESSAGE QUEUE 86
CACHE SUBSYSTEM 78
CUSTOMER 90
ROUTING 96
POLICY 92
LOCATION 98
DOMAIN 94
CACHE MANAGER 100
HANDLER SUBSYSTEM 80
AUTHENTICATION 102
ACCOUNTING 104

Fig. 4

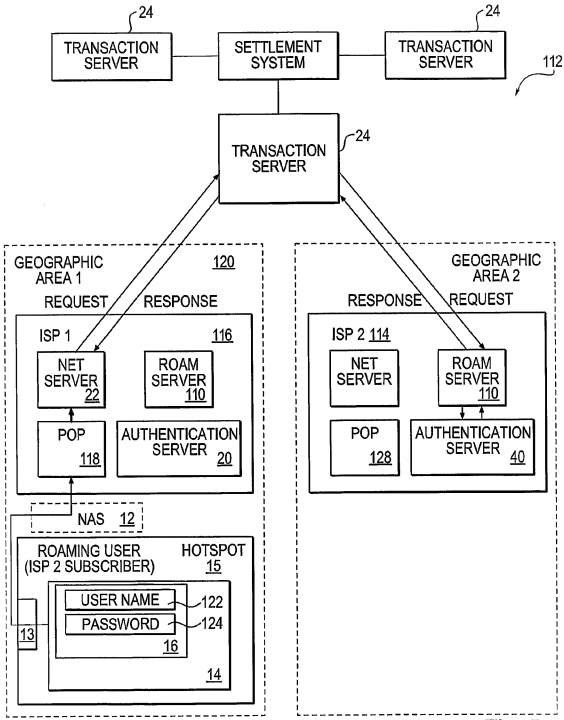

24
TRANSACTION SERVER
SETTLEMENT SYSTEM
24
TRANSACTION SERVER
112
TRANSACTION SERVER
24
GEOGRAPHIC AREA 1
120
REQUEST
RESPONSE
ISP 1
116
NET SERVER 22
ROAM SERVER 110
POP 118
AUTHENTICATION SERVER 20
NAS 12
ROAMING USER (ISP 2 SUBSCRIBER)
HOTSPOT 15
USER NAME
122
PASSWORD
124
16
13
14
GEOGRAPHIC AREA 2
RESPONSE
REQUEST
ISP 2 114
NET SERVER
ROAM SERVER 110
POP 128
AUTHENTICATION SERVER 40

Fig. 5

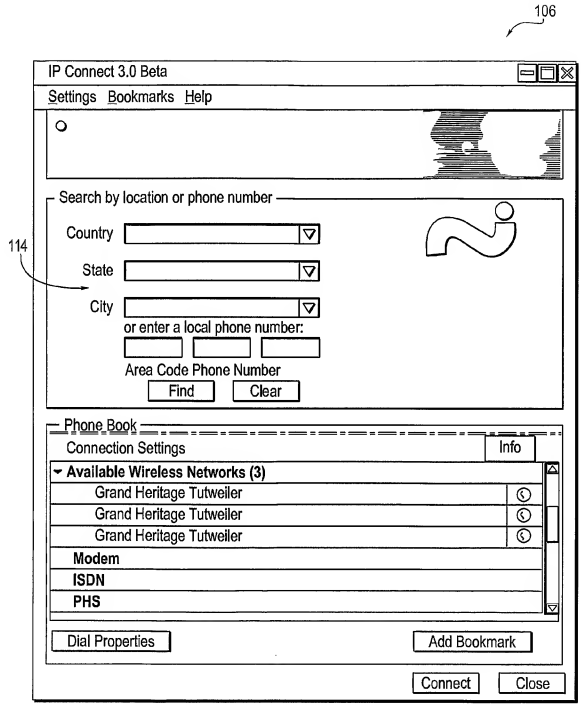

106
IP Connect 3.0 Beta
Settings Bookmarks Help
Search by location or phone number
114
Country
State
City
or enter a local phone number:
Area Code Phone Number
Find
Clear
Phone Book
Connection Settings
Info
Available Wireless Networks (3)
Grand Heritage Tutweiler
Grand Heritage Tutweiler
Grand Heritage Tutweiler
Modem
ISDN
PHS
Dial Properties
Add Bookmark
Connect
Close

Fig. 6

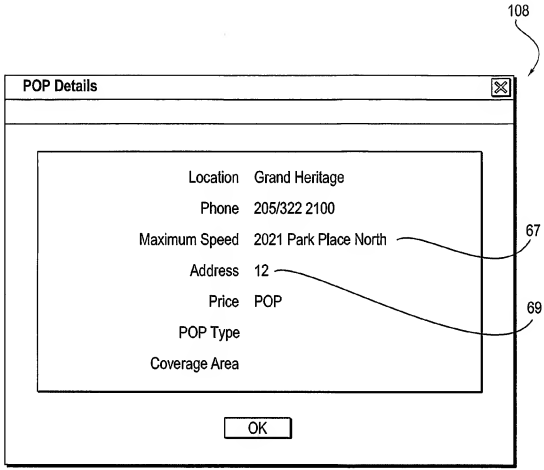

108
POP Details
Location Grand Heritage
Phone 205/322 2100
Maximum Speed 2021 Park Place North
Address 12
Price POP
POP Type
Coverage Area
67
69
OK

Fig. 7

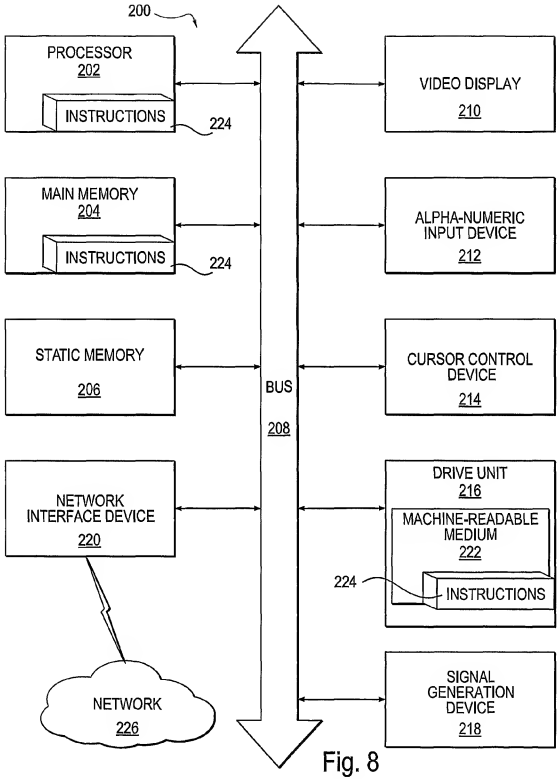

200
PROCESSOR
202
INSTRUCTIONS
224
MAIN MEMORY
204
INSTRUCTIONS
224
STATIC MEMORY
206
NETWORK
INTERFACE DEVICE
220
NETWORK
226
BUS
208
VIDEO DISPLAY
210
ALPHA-NUMERIC
INPUT DEVICE
212
CURSOR CONTROL
DEVICE
214
DRIVE UNIT
216
MACHINE-READABLE
MEDIUM
222
224
INSTRUCTIONS
SIGNAL
GENERATION
DEVICE
218

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/17905

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173, 15/16, 11/30
US CL : 709/223, 227, 229; 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/203, 219, 223, 227, 229, 237; 705/64; 713/182, 189, 200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,369,705 A (BIRD et al) 29 November 1994 (29.11.1994); abstract; Fig. 1-4, 8, 9; col. 1, line 1 - col. 3, line 10; col. 3, line 45 - col. 4, line 5; col. 15, line 25 - col. 17, line 15	1-5, 8, 9, 12-20, 22, 24-28, 31, 32, 34-36 --- 6, 7, 10, 11, 21, 23, 29, 30, 33
Y	US 6,233,446 B1 (DO et al.) 15 May 2001 (15.05.2001); abstract; Fig. 1-7; col. 1, line 1 - col. 2, line 30; col. 3, line 25	7, 23, 30
Y	US 2003/0039237 A1 (FORSLOW) 27 February 2003 (27.02.2003); abstract; Fig. 1-4, 8-13; Page 1, 0001 - Page 4, 0034	6, 10, 11, 21, 29, 33
Y	US 6,298,234 B1 (BRUNNER) 02 October 2001 (02.10.2001); abstract; Fig. 1-3; col. 1, line 1 - col. 3, line 5; col. 3, line 30 - col. 4, line 55	1-36
Y	US 6,449,722 B1 (WEST et al) 10 September 2002 (10.09.2002); abstract; Fig. 1-3; col. 1, line 1 - col. 2, line 35; col. 2, lines 50-60	1-36
A	US 6,338,140 B1 (OWENS et al) 08 January 2002 (08.01.2002); abstract, Fig. 1-6, 8-11; col. 1, line 1 - col. 12, line 35	1-36
A	US 6,466,964 B1 (LEUNG et al) 15 October 2002 (15.10.2002); abstract; Fig. 1-3, 7-9, 13; col. 1, line 1 - col. 4, line 30	1-36

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 September 2003 (05.09.2003)	14 OCT 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Rupal Dharia Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US03/17905

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,571,095 B1 (KOODLI) 27 May 2003 (27.05.2003); abstract; Fig. 1-5; col. 1, line 1 - col. 5, line 40	1-36